General Data Protection Regulation (GDPR) Policy Statement

Steadline Ltd is committed to a policy of protecting the rights and privacy of individuals, including full and part time staff, suppliers, members of the public and all relevant others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how companies manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that Steadline need to be aware of as data controllers, including provisions intended to enhance the protection of full and part time staff's personal data.

Steadline have populated a Data Protection Compliance matrix, which details the various forms of personal data retained on staff, additional information will be held on suppliers and clients with their permission including but not limited to:

- Credit and financial history
- Insurances and Health and Safety policies
- Personnel information, contact numbers, email addresses
- Certain accreditations such as RISQS, SSIP, ISO information
- Training records of staff from Labour agencies or recruitment companies

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR), Steadline will ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff and suppliers. Any breach of this policy or of GDPR itself will be considered a breach and the company's disciplinary procedures will be invoked. As a matter of best practice, other individuals working with Steadline and who have access to personal information, will be expected to read and comply with this policy. It is expected that personnel who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

This piece of legislation came into force on the 25th May 2018. The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example, by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be

in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

Responsibilities under the GDPR

Steadline will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. Steadlines Managing Director has also been appointed as the Data Protection Officer (DPO) who is available to address any concerns regarding the data held and how it is processed, held and used.

Individuals who provide personal data to Steadline are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, Steadline undertakes to adhere to the eight principles:

1. **Process personal data fairly and lawfully.**

Steadline will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. **Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.**

Steadline will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. **Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.**

Steadline will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data is provided by individuals, this such data will be destroyed immediately.

4. **Keep personal data accurate and, where necessary, up to date.**

Steadline will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify Steadline if, for example, a change in circumstances means that the data needs to be updated. It is the responsibility of Steadline to ensure that any notification regarding the change is noted and acted on.

5. **Only keep personal data for as long as is necessary.**

Steadline undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Steadline will undertake a regular review of the information held and implement a weeding process. Steadline will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6. Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- be told the nature of the information Steadline holds and any parties to whom this may be disclosed to.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision-making process that will significantly affect them.

Steadline will only process personal data in accordance with the rights of those individuals.

7. Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All Steadline members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. Steadline will ensure that all personal data is accessible only to those who have a valid reason for using it.

Steadline will have in place appropriate security measures for ensuring that hard copy personal data is securely stored with controlled access, which may include:

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinets).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, Steadline will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed. This policy also applies to staff who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8. Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Steadline will not transfer data to such territories without the explicit formal consent of the individual. This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so Steadline will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If Steadline collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Consent as a basis for processing
Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when Steadline is processing any sensitive data, as defined by the legislation. Steadline understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Policy & Process Review
Steadline will ensure that this Policy and all processes that are referred to for the management and control of data shall be subject to regular monitoring and review. Monitoring is to ensure that the data management and control processes are being effectively implemented and adhered to. Review is to ensure that our Policy and processes remain valid, up to date, relevant, compliant with legislation and take into account any opportunity for improvement.

Kevin Gray 24th February 2022

Managing Director & Data Protection Officer